ORDER FOR SUPPLIES AND SERVICES	IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution	PAGE 1 OF 1 PAGE(S)

1. DATE OF ORDER	2. ORDER NUMBER	3. CONTRACT NUMBER	4. ACT NUMBER
08/29/2011	GST0311DS7042	GS-06F-0524Z	A2473397H

FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 299X	ORG CODE A03VR110	B/A CODE F1	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE C01	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT

7. TO: CONTRACTOR *(Name, address and zip code)*	8. TYPE OF ORDER	REFERENCE YOUR
Vic Blanco AMERICAN VETERANS LLC 2 Brittany Ln Stafford, VA 22554-7687 United States (b) (6)	B. DELIVERY	
	Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.	
	This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.	
	C. MODIFICATION NO. 00 TYPE OF MODIFICATION:	AUTHORITY FOR ISSUING

9A. EMPLOYER'S IDENTIFICATION NUMBER	9B. CHECK, IF APPROP WITHHOLD 20%	
202925557		Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.

10A. CLASSIFICATION	10B. TYPE OF BUSINESS ORGANIZATION
A. Small Business	C. Corporation

11. ISSUING OFFICE *(Address, zip code, and telephone no.)*	12. REMITTANCE ADDRESS *(MANDATORY)*	13. SHIP TO*(Consignee address, zip code and telephone no.)*
GSA Region 3 Eileen S. Flanigan 20 North Eighth Street Philadelphia, PA 19107-3191 United States (b) (6)	AMERICAN VETERANS LLC 2 Brittany Lane Stafford,VA 22554 United States	Doris Stevenson-Burton 810 Vermont Ave. NW. (005F2) Washington, DC 20420 United States (b) (6)

14. PLACE OF INSPECTION AND ACCEPTANCE	15. REQUISITION OFFICE *(Name, symbol and telephone no.)*
Doris Stevenson-Burton 810 Vermont Ave. NW. (005F2) Washington, DC 20420 United States	Allen Cardwell GSA Region 3 20 North 8th Street Philadelphia, PA 19107 United States (b) (6)

16. F.O.B. POINT	17. GOVERNMENT B/L NO.	18. DELIVERY F.O.B. POINT ON OR BEFORE	19. PAYMENT/DISCOUNT TERMS
Destination		08/28/2012	NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS

20. SCHEDULE

This task order (GST0311DS7042) is hereby awarded to American Veterans, LLC for Enterprise Architecture Support for the 16 Major Initiatives (EAS 16) for the Department of Veteran's Affairs Office of Technical Architecture and Innovation (TA&I). The Government's Performance Work Statement is referenced under ITSS order R3114402. American Veterans LLC's cost quote dated 06/03/2011 is accepted.
The total estimated Time and Material amount in the Base Year is (b) (4) .
The base year period of performance begins on 08/29/2011 and ends on 08/28/2012. The PWS and Quality Assurance Surveillance Plan are hereby incorporated.

This task order is fully funded in accordance with FAR Clause 52.232-22 entitled "Limitation of Funds". Funding in the amount of $5,683,263.35 is provided to fully fund the base period for the Contractor performance. The Contractor is not authorized to exceed this amount unless authorized by the GSA Contracting Officer.

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	Base Year EAS16 (includes labor and travel CLINS per Price Sheet)	1	lot	(b) (4)	(b) (4)

21. RECEIVING OFFICE *(Name, symbol and telephone no.)*	TOTAL From 300-A(s)	
Principal DAS for Information and Technology, (202) 461-4339		
22. SHIPPING POINT Specified in QUOTE	23. GROSS SHIP WT.	GRAND TOTAL $5,683,263.35
24. MAIL INVOICE TO: *(Include zip code)* Finance Operations and Disbursement Branch (BCEB) 299X PO Box 219434 Kansas City, MO 641219434 United States	25A. FOR INQUIRIES REGARDING PAYMENT CONTACT: GSA Finance Customer Support	25B. TELEPHONE NO. (b) (6)
	26A. NAME OF CONTRACTING/ORDERING OFFICER*(Type)* Eileen S. Flanigan	26B. TELEPHONE NO. (b) (6)

Department of Veterans Affairs (VA)
Office of Information & Technology (OI&T)
Office of IT Architecture Strategy and Design (ASD)
Technical Architecture & Innovations

PERFORMANCE WORK STATEMENT (PWS)

Enterprise Architecture Support for the "16 Major Initiatives for the VA" (EAS16)

EAS16 - Table of PWS Revisions

Rev. No.	Rev. Date	Name	Description	TO Mod No.
1	05/23/2011	A Cardwell	**5.6 Place of Performance** - Added: "The Government will not be responsible for the cost for daily on-the-job / local travel. **4.3.3 SCHEDULE FOR DELIVERABLES** - changed 1st entry in table to indicate that only a single PMP is required for this task order.	Amend 3
2	05/26/2011	A Cardwell	**5.6 Place of Performance** - Changed references to point to Section 4. **4.3.3 SCHEDULE FOR DELIVERABLES** – changed all references from Section 3.1.1 to 3.2.1 **4.3.3 SCHEDULE FOR DELIVERABLES** – changed entries for Program Communication Plan, and for Risk Management Plan, to indicate that there is one required for each Major Initiative. **3.3 Enterprise Architecture and Innovation** – removed the following artifacts from lists: 'Service Registry', 'SOA Repository', 'Target State' and 'Enterprise Systems Model'	Amend 4
3	04/13/2012	A Cardwell	Added the following sections: **3.4.4 EA Tool Suite Assessment and Recommendation** **3.4.5 Develop Enterprise Modeling Standards** Updated the related deliverables in Section: **4.4.3 SCHEDULE FOR DELIVERABLES** Note: Mod 01 also includes a reallocation of labor hours.	Mod 01
4	10/03/2012	A Cardwell	**4.5 GOVERNMENT FURNISHED PROPERTY –** added GFP clause based on new VA requirement for OneVA EA program development effort. **3.3.2 Across all VA Major Initiatives the Contractor shall –** added this requirement and deliverables	Mod 05

			4.3.3 SCHEDULE FOR DELIVERABLES – Updated table to include deliverables defined in added **Section 3.3.2**	
5	12/11/2012	A Cardwell	**5.3 TASK ORDER CONTACT INFO** – Tracy Pham designated as COR **<<Current Updates Highlighted in Yellow>>**	Mod 006

1.0 GENERAL INFORMATION

1.1 TYPE OF TASK ORDER –LABOR HOURS

1.2 BACKGROUND

The Office of Technical & Business Architecture (T&BA) is positioned organizationally in the Architecture Design & Strategy (ASD) Office within the VA Office of information and Technology (OI&T) and serves as the Enterprise Architecture Office for the VA. T&BA provides guidance, standards, and governance for developing and maintaining the VA Information Technology (IT) enterprise architecture. T&BA partners with Administration and VA Staff Office architects, business owners, and project managers to leverage the VA IT enterprise architecture to provide data services support, modeling development, systems & process analysis, and architectural governance support. Provision of this type of support enables the VA IT enterprise architecture to serve as a key tool that facilitates and drives sound business-oriented information technology choices.

The VA Secretary has identified 16 major initiatives representing the highest priorities for the Department to achieving its mission. T&BA is tasked with providing IT Enterprise Architecture (EA) Support for these "16 Major Initiatives for the VA." This task of providing EA support includes developing and implementing architectures using the OneVA Enterprise Architecture approach and EA Governance. The OneVA approach was directed by the VA Secretary as a way of operationally realizing the concept that the agencies of the VA are one entity. The OneVA policy is found in VA Directive 6051 and the technical approach is found in the OneVA Enterprise Architecture Guidance. All VA IT architecture descriptions are to be developed with the purpose and vision of the OneVA approach in mind.

Currently, various initiative programs supporting these Major Initiatives are in progress and are making important design decisions that influence how the overall IT architecture of the VA as an enterprise evolves. These programs operate at varying levels of maturity in how decisions are made and solutions are built. The solution for this acquisition needs to be able to work in an agile fashion while ensuring that the VA enterprise infrastructure grows in an integrated fashion. This ensures EA outputs to be actively used by all major initiatives teams and not be relegated to being a set of documentation shelf ware.

This acquisition solution will provide EA support to the Major Initiatives. These initiatives are part of VA's overarching strategy to pursue the President's two overarching goals for the Department which are to transform VA into a 21st Century organization and to ensure that we provide timely access to benefits and high quality care to our Veterans over their lifetimes, from the day they first take their oaths of allegiance until the day they are laid to rest. The Major Initiatives are:

1. **Eliminate Veteran Homelessness (EVH)**
   The goal of this initiative is to end homelessness among our nation's Veterans. VA will assist every eligible homeless Veteran willing to accept services.

2. **Enable 21st century benefits delivery and services (e.g., backlog reduction) (Veterans Benefits Management System - VBMS)**

The goal of this initiative is to provide a world-class paperless environment for veteran claims processing and benefits delivery across the five VBA business lines: C&P, Education, Vocational Rehabilitation and Employment, Insurance, and Loan Guaranty.

3. **Automate GI Bill benefits (GIBILL)**
   The goal of this initiative is to implement the business processes and automation to provide a client-centered approach to delivering the education benefits provided under the Post-9/11 GI Bill.

4. **Implement Virtual Lifetime Electronic Records (VLER)**
   The goal of this initiative is to provide a visionary, interagency federal initiative, in collaboration with the private sector, to create a secure exchange for electronically sharing and proactively identifying the entire spectrum of health and benefits entitlements for our service members and veterans, and for their dependents and registered agents where applicable and appropriate, from accession through final honors.

5. **Improve Veteran mental health (IVMH)**
   The goal of this initiative is to transform VA mental health programs into a subsystem operating within the larger VHA health care system, which is self-regulating, patient-centered, and offers meaningful choices to Veterans (and families).

6. **Build Veteran Relationship Management (VRM) capability to enable convenient, seamless interactions**
   The goal of this initiative is to provide the capabilities required to achieve on-demand access to comprehensive VA services and benefits in a consistent, user-centric manner to enhance Veterans, their families, and their agents' self-service experience through a multi-channel customer relationship management approach. This initiative is designed to improve the speed, accuracy, and efficiency in which information is exchanged between Veterans and the VA, regardless of the communications method (phone, web, email, social media).

7. **Design a Veteran-centric healthcare model and right-sized infrastructure to help Veterans navigate the health care delivery system and receive coordinated care (New Health Care Model – NHCM)**
   The goal of this initiative is to develop and implement new models of care that educate and empower patients and their families, focus not only on the technical aspects of care but ensure a more holistic, Veteran centered system, and greatly improve access and coordination of care.

8. **Expand health care access for Veterans, including women and rural populations (ACCESS)**
   The goal of this initiative is to eliminate disparities in access to care wherever they exist within our system.

9. **Ensure preparedness to meet emergent national needs (e.g., hurricanes, H1N1 virus) (Integrated Operations Center – IOC)**
   The goal of this initiative is to build and maintain the capabilities required to enable continued services to Veterans regardless of conditions by driving Continuity of Government (COG), and Continuity of Operations (COOP) Programs.

10. **Develop capabilities and enabling systems to drive performance and outcomes (Enterprise Wide Cost Accountability – EWCA)**
    The goal of this initiative is to identify and define the Department's cost information requirements for managerial decision making.

11. **Establish strong VA management infrastructure and integrated operating model (IOM)**
    The goal of this initiative is to focus on the development of an enhanced management infrastructure and integrated operating model (IOM) that will improve the integration and management within and across the Department's five key corporate management functions: Construction and Facilities Management, Financial Management, Acquisitions, Information Technology and Human Resources Management.

12. **Transform human capital management (Human Capital Improvement Plan - HCIP)**
    The goal of this initiative is to develop the VAs human capital into a proactive, forward looking, and professional workforce. This will include a focus on improving recruiting, hiring, and retention; investing in people development (e.g., leadership training); better supporting and developing the capabilities of our Senior Executive Service (SES); and striving to build a broad set of Human Resources capabilities.

13. **Perform research and development (R&D) to enhance the long-term health and well-being of Veterans**
    The goal of this initiative is to discover knowledge, develop VA researchers and health care leaders, and create innovations that advance health care for our Veterans and the nation.

14. **Strategic Capital planning**
    The purpose of this initiative is to capture the full extent of VA infrastructure and service gaps and to develop both capital and non-capital solutions to address these gaps by 2021. The SCIP process is a 21st century transformative tool which will enable VA to deliver the highest quality healthcare, benefits, and memorial services to our Nation's Veterans through investing in the future and improving efficiency of operations.

15. **Health Care Efficiency (HCE)**
    The purpose of this initiative is to, reduce, or eliminate organizational variation in business and clinical areas. HCE's initial focus is in the areas of Commodity Standardization, Non-VA Care, Accreditation, Beneficiary Travel, Specific Purpose Funded Programs and Facilities Automation. Eliminating unwanted variation will reduce health care operational costs and create a more streamlined deployment of targeted programs to enhance program efficiency across VHA.

16. **Transforming Health Care Delivery through Health Informatics**
    This Initiative transforms health care delivery to Veterans by delivering informatics solutions that will directly improve information quality and accessibility while optimizing value. Additionally, it ensures that VA regains and continues industry leadership in the use of health informatics and health information technology. This Initiative will serve as a foundational component for VA's transition from a medical model to a patient-centered model of care. It requires cultural, informational, and technological paradigm shifts to implement a sophisticated electronic health management platform supporting cognition, communication and workflow of patients and clinicians while ensuring compatibility with

other non-VA systems and partners. Products of the Initiative are grouped within work streams focused on revitalizing development, enhancements to the electronic clinical environment, building informatics capacity, and managing the future through deliberate application of health IT and informatics.

EA support for these 16 major initiatives form the tasking identified in this Performance Work Statement (PWS) and collectively will provide for the continued development, maintenance and implementation of a OneVA EA using the Department's 16 Major Initiatives to transform VA. Currently there are 16 major initiatives but this number may change over the course of this acquisition. This task order covers EA work associated with all designated VA Major Initiatives.

2.0 SCOPE OF WORK

The various programs supporting the 16 Major Initiatives are in progress and are making important design decisions that influence how the overall architecture of the VA as an enterprise evolves. These programs operate at varying levels of maturity in how decisions are made and solutions are built.

The Contractor Team shall work in an agile fashion to sustain and enhance the current level of EA service provided to the VA Major Initiatives, and be responsive to VA business and organizational needs as it pertain to EA support and other information technology (IT) engineering related disciplines in support of the VA enterprise and business lines missions. This Contractor team shall also provide T&BA with expert knowledge of enterprise architectural development and implementation and IT enterprise infrastructure and technologies. EA Contractor Team shall support the EA activities of the "16 Major Initiatives of the VA." Supporting the EA activities requires the knowledge of all available enterprise architecture artifacts including multiple architectural models or views that show how the current and future needs of the initiatives will be met in an efficient, sustainable, agile, and adaptable manner.

The EA Contractor Team shall have expert knowledge of Federal Enterprise Architecture (FEA) Reference Models, Federal Segment Architecture Methodology (FSAM), other enterprise architecture best practices such as Department of Defense Architecture Framework (DoDAF), and architecture modeling tools.

The specific deliverables for each of the "16 Major initiatives of the VA" are not currently known. These will be established as part of the initial EA work for each major initiative. Nearly all deliverables for each initiative will be drawn from the list established later in the PWS. However, there may be EA artifacts that the contractor will be required to develop that are not currently known.

This PWS describes the required skills and tasks necessary to fulfill the goals of this task order. It lists the known deliverables, categorizing them as to the level of effort necessary for their development. In addition, the RFQ includes guidance on the level of effort necessary to fulfill the TO requirements. This information will assist the contractor in developing their labor hour quote. However, regardless of the degree to which this information enhances the ability to accurately estimate the required level-of-effort necessary for this task order, anticipated changes to priorities and new Enterprise Architecture requirements that fall within the task order scope will need to be addressed and will consequently challenge available resource availability. The Government's plan to deal with these events is to work within the level of effort established by this task order, by putting lower priority requirements on hold, focusing the contractor's effort on the highest Government priorities. However, the quantity of high

priority requirements could increase beyond the ability of the established level of effort to address. If this circumstance should develop the Government will expand the task order level of effort as necessary to address the dynamic aspect of this requirement.

3.0 SKILLS, TASKS & DELIVERABLES

3.1 REQUIRED SKILLS

3.1.1 Enterprise Architecture

The EA support for the 16 Major Initiatives needs high level support to align IT strategy and planning with the Major Initiative business goals; explain complex technical issues in a way that non-technical people may understand; have Knowledge of IT governance and operations; work with our most senior executives & architects to understand their highest priority business needs; work with Major Initiatives Leads to align technology to their most critical business opportunities and needs; align with and support ASD standard architecture products; ensure proper business value and in quality project deliverables; and ensure technical decisions align with the customer's business and provide value. A major aspect of enterprise architecture support is prescribing architecture artifacts for the individual Major Initiatives.

3.1.2 Project Management

This task order requires support for all aspects of project management including technical oversight, documentation tracking, governance, and project leadership. Included are management of project scope, reviews, meetings, work assignments, reporting, status and other related project oversight responsibilities. Some specific PM accountabilities:

a) Updating the OneVA EA Guidance quarterly as needed

3.1.3 Documentation Support

The EA support for the 16 Major Initiatives needs technical support for the creation of documents. These deliverables include project artifacts such as work product review notes, meeting notes, and user documentation. Support will be required throughout the project period of performance.

3.1.4 Data Architecture Support

The EA Support for Major Initiatives needs development support for both Logical and Physical Data Modeling. The data architects shall develop and maintain a formal description of the data and data structures - this can include data definitions, data models, data flow diagrams, etc. (in short; metadata). These architecture artifacts are the key deliverables of this task order.

3.1.5 Subject Matter Expertise (Architecture & Business Analysis)

The EA Support for Major Initiatives needs Subject Matter Expertise in the area of Architecture & Business Analysis. This support will provide expert support to identify and translate system requirements into software design documentation, act as visionary and strategist for solution product area, work with technical writers to ensure quality internal and external client-oriented documentation, and work very closely with developers to ensure proper implementation of products. SME's shall also interface and coordinate tasks with internal and external technical resources. Collaboration with Project Managers and technical leaders is required to provision estimates, develop overall implementation solution plan, and to serve as lead as required, to implement installation, customization, and integration efforts

3.2 SPECIFIC TASKS

3.2.1 Project Management

3.2.1.1 Project Management Plan

The Contractor shall draft a Project Management Plan (PMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS.

The PMP will be used establish and maintain the due dates for deliverables for all program activities. These shall be approved by the VA TOPM, and be the basis for tracking contractor performance throughout the task order period of performance.

The initial baseline PMP shall be reviewed and approved by the VA TOPM and updated monthly thereafter.

Deliverables:

A. Project Management Plan

3.2.1.2 Kick-off Requirements

The Contractor shall:

a) Hold a Project Kick-Off Meeting with a project advisory group comprised of key stakeholders and subject matter experts (SMEs). Schedule the Kick-Off Meeting within ten (10) business days after contract award, or as agreed upon between T&BA and the Contractor. Stakeholders and SMEs will be identified by T&BA following contract award, but NLT 24 hours prior to a scheduled meeting;

b) Present the details of their intended approach, work plan and project schedule, including preliminary deliverable dates for reviews, to the VA TOPM. Work shall not commence until the VA TOPM approves the approach / methodology of the Contractor, a preliminary work plan, and schedule

Deliverables:

A. Staff Rosters
B. Completion of Project Kick-Off Meeting
C. Minutes of Project Kick-Off Meeting
D. Project Work Plan Presentation

3.2.1.3 Communication Planning

The Contractor shall maintain a Program Communication Plan for each of the 16 Major initiatives specified in Section 1.2. Contractor shall:

a) Develop, maintain, and execute a Program Communication Plan (PCP). The PCP is a written document that describes when, where and how Contractor personnel will interact and

communicate with the broader VA enterprise to further the objectives of the OneVA architecture effort. The PCP may suggest the use of newsletters, e-mail, company intranet, meetings and events, teleconferences, bulletins and other special communications projects, as appropriate to convey project information throughout the enterprise. The PCP shall also include a strategy for setting and managing appropriate customer expectations. Additionally, the means by which the results of executing the PCP will be assessed and evaluated to determine its effectiveness shall be included.

b) Ensure that the PCP is applicable across all 16 Major Initiatives, and includes an understanding of the different audiences within the various Initiatives. There shall be coordination of communications/messaging across all 16 Initiatives

c) Develop both external and internal communication processes to manage information across and within Initiatives and partner organizations

Deliverables:

A. Program Communication Plan

3.2.1.4 Risk Management

The Contractor shall:

a) Develop, maintain and implement a project Risk Management Plan (RMP) for each of the 16 initiatives. The RMP identifies knowable circumstances that may have a negative impact on the enterprise architecture, describes these potential impacts, and asserts measures to either reduce/eliminate their potential or minimize their impact;

b) Collaborate with project stakeholders to prioritize, scope, bound, resource and assess course of actions related to program risks. The Contractor shall inform the VA TOPM and applicable project stakeholders of relevant deliberations and the Contractor's recommendations;

c) Work to mitigate and resolve program risks as they are identified. The Contractor shall report all risk items and their disposition in the MPR.

Deliverables:

A. Risk Management Plan
B. Risk Status Tracking and Mitigation Reports

3.2.1.5 Change Control

The Contractor shall:

a) Update, document, and execute a Configuration Management Plan (CMP) for each of the 16 initiatives. The CMP is a document that specifies the Change Control Process and the lifecycle management of EA artifacts. Change Control consists of the formal procedures used to ensure that changes are executed in a controlled and coordinated manner. Artifacts include architecture models, information documents, Business Process Models, and developed applications referenced in this PWS;

b) Document the Change Control Process (CCP) as a business process in a Configuration Management Plan. The CCP shall be inclusive of a Change Control Board (CCB) with government representation. The CCB will have authority over project deliverable changes as part of the CCP.

c) Support the CCB via the establishment and coordination of CCB meetings, recording of CCB minutes, capture of change proposals, and the participation in program discussions. The CCB shall operate IAW the CCP defined in the CMP. CCB sessions shall be documented via meeting minutes, and appropriate changes via engineering change proposals.

Deliverables:

A. CMP w/Change Control Process
B. CCB Meeting Minutes
C. Engineering Change Summaries

3.2.1.6 Enterprise Architecture Working Group (EAWG)

The Contractor shall:

a) Facilitate and participate in an EA WG. The purpose of the EA WG is to review key project activities and topics, summarize their effects, and identify potential future course of action. The Contractor shall develop an EA WG Charter that supports this effort;

b) Facilitate EA WG meeting on a twice-monthly basis or other routine basis. EA WG activities and topics may include project accomplishments, potential lessons learned, risk items and mitigation approaches, findings of technical assessments, technical planning, and quality improvement initiatives. EA WG meeting shall also be used as a forum to identify opportunities for project improvement in any and all areas.

Deliverables:

A. EA WG Charter
B. Minutes of EA WG Meetings

3.2.1.7 Integrated Product Team (IPT)

The Contractor shall:

a) Participate in monthly IPT meetings for each assigned major initiative (i.e. 16 Major Initiatives for the VA). Provide architecture expertise to the activities of the IPT. The purpose of the IPT, which consist of a cross-functional team, is to procure major acquisitions. The IPT should work collaboratively to develop strategies and approaches to meet specific acquisition and program objectives;

a) Represent the EA team in the IPT meetings. Identify impacts to the OneVA Enterprise by summarizing the effects and making recommendations. IPT activities may include defining and refining the technical requirements; Discussing risks and developing mitigation strategies; and determining the optimal acquisition strategy.

Deliverables:

A. Minutes of IPT Meetings

B. Written Recommendations

3.2.2 Reporting Requirements

a) **Weekly Activity Report -** Provide weekly activity reports for each project to the VA TOPM;

b) Monthly Progress Report (MPR) -

The Contractor shall submit a written Monthly Status Report to the VA TOPM and the GSA COTR on the 5th day of each month. Information included in the MPR shall be segregated in accordance with a Government approved format. As a minimum, the Monthly Progress Report shall include:

- Contract number and Task Order number
- A narrative review of work accomplished and significant events occurring during the reporting period, segregated by PWS task areas
- Description of the status and progress in completing artifacts/deliverables
- Identification of risks, issues, or problems encountered with corrective actions taken and recommendations to mitigate or resolve
- Anticipated activity for the next reporting period
- Staffing levels and vacancies, including personnel gains/losses/status of hiring activities
- Adjustments to schedules, if any, shall be explained
- Summary of Ad-hoc Technical Reports provided.
- Description of any travel or unique services:
- Travel summary shall include, at a minimum, describe the travel conducted, including a statement as to purpose, the number of persons in the party, traveler name(s), destination(s), duration of stay, and estimated and/or actual cost.
- Summarize meetings attended, major outcomes or issues discussed, and any action items.
- Identify planned travel for the coming month: include a statement as to purpose, the number of persons in the party, traveler name(s), destination(s), duration of trip, and estimated cost.

The Contractor shall notify the VA TOPM, GSA COTR, and CO, in writing, immediately if problems arise adversely impacting the performance of the PWS.

Deliverables:

A. Weekly Activity Reports
B. Monthly Progress Report

3.3 Enterprise Architecture and Innovation

The "16 Major Initiatives for the VA" are aligned with missions of the VA Business Lines. The Contractor shall support these initiatives by developing and/or enhancing enterprise architecture products such as the following five FEA reference models:

1) Performance Reference Model (PRM)
2) Business Reference Model (BRM)
3) Service Component Reference Model (SRM)
4) Technical Reference Model (TRM)
5) Data Reference Model (DRM)

Update the OneVA EA Guidance as needed. Contractor architects, technical writers, business analysts, project coordinators, and technicians shall adhere to this when developing or maintaining EA components, IT services or segments of the OneVA EA. This guide outlines the EA governance process.

Conduct bi-annual studies on EA best practices, EA modeling tools, and EA presentation techniques. These assessments and studies are quick market surveys and evaluations of available technologies that may be relevant to executing the One-VA IT architecture and other IT services.

Update and provide written recommendations to the VA TOPM regarding the Future IT Architecture Vision (FAV). The Future IT Architecture Vision provides a view of what is technologically possible on an implementation-horizon somewhat beyond the seven-year implementation-horizon established for the Target IT architecture Vision. The FAV shall be maintained via quarterly updates.

3.3.1 For each of the Major Initiatives, the Contractor shall:

- Develop or update BPMs and narratives, and provide written recommendations to the VA TOPM on business process re-engineering of VA business lines. BPMs (As-Is and To-Be models) are developed or updated monthly as established by the VA TOPM.
- Develop and/or Update Transition Sequencing Plan and associated IT architecture products as specified by the VA TOPM, inclusive of Project Deployment Timelines, Transitions Lists and Transition Performance Measure. The Transition Sequencing Plan identifies the activities and sequence of execution necessary to achieve the Target IT architecture end state starting from As-Is IT architecture state. The Target Sequencing Plan integrates established IT development projects, along with proposed projects suggested by the Target Gap Analysis into a deployment timeline.
- Update the Gap, Redundancy and Reuse Analysis of the As-Is OneVA Target EA. The Gap, Redundancy, and Reuse Analysis identifies the investments and adjustments beyond those identified in the target IT architecture transition plan, that are required to move the VA As-Is EA state to the VA Target EA state. Gap Analysis shall be maintained via monthly updates.

Possible Deliverables for each of the 16 Major initiatives:

These may be in both “As-Is” and “To Be” artifacts/models. Further details can be found in FSAM and FEA.

The following is a list of possible EA artifacts deliverables that may be required for each of the 16 Major Initiatives. The specific artifacts for each Major Initiative are not known and will be determined based on the specific requirements of each Initiative. This list is divided into 3 major categories (i.e. Small, Medium and Large) according to the estimated level-of-effort required to create the listed artifact.

<u>Small</u> (< 100 hours to create)

Business Requirements
IT Infrastructure (HW, Networks) Architecture
Mappings / Traceability to Business Components
Service Inventory

Software Architecture Document (SAD)
Software Design Document (SDD)
Systems Architecture Description
Technical Standards Viewpoint
Transition Sequencing Plan
Use Cases (Synchronous and Asynchronous)
Application to Data Relationships
Applications Architecture
Communications Plan
Interface Catalog
Security Architecture
System Design Document
UML Component Diagram
Business Process Model
Business Service Model (leads to "Service Inventory")
Deployment Diagram
Sequence Diagram
SOA Guidance
System Interface Diagram
UML Deployment Diagram
StdV-1 Standards Profile
SV-9 Systems Technology & Skills Forecast
AV-1 Overview and Summary Information
CV-5: Capability to Organizational Development Mapping
DIV-1: Conceptual Data Model
OV-1: High-Level Operational Concept Graphic
PV-1: Project Portfolio Relationships
PV-2: Project Timelines
CV-2: Capability Taxonomy
CV-3: Capability Phasing
CV-7: Capability to Services Mapping
OV-4: Organizational Relationships Chart
OV-6b: State Transition Description
SV-8 Systems Evolution Description
SvcV-1 Services Context Description
SvcV-10a Services Rules Model
SvcV-10c Services Event-Trace Description
SvcV-2 Services Resource Flow Description
SvcV-3b Services-Services Matrix
SvcV-5 Operational Activity to Services Traceability Matrix
SvcV-6 Services Resource Flow Matrix

SvcV-7 Services Measures Matrix
SvcV-9 Services Technology & Skills Forecast
AV-2 Integrated Dictionary
CV-1: Vision
StdV-2 Standards Forecast
SV-1 Systems Interface Description
SV-2 Systems Resource Flow Description
SV-3 Systems-Systems Matrix
SV-5a Operational Activity to Systems Function Traceability Matrix
SV-5b Operational Activity to Systems Traceability Matrix
SV-7 Systems Measures Matrix
SvcV-10b Services State Transition Description
SvcV-3a Systems-Services Matrix
SvcV-8 Services Evolution Description

Medium (between 100 and 200 hours to create)

Business Rules
Functional Requirements
Gap Analysis
Interface Control Document (ICD)
Service Level Agreement (SLA) (aka Business Non-Functional Requirements)
Systems Model
Technical Requirements
User Interfaces/User Experience Models
Class Diagram
Data Model
Data to IT Infrastructure
Information Model
OV-6a: Operational Rules Model
OV-6c: Event-Trace Description
PV-3: Project to Capability Mapping
SV-10a Systems Rules Model
SV-10b Systems State Transition Description
SV-6 Systems Resource Flow Matrix
SvcV-4 Services Functionality Description
CV-4: Capability Dependencies
CV-6: Capability to Operational Activities Mapping
OV-2: Operational Resource Flow Description
OV-5a: Operational Activity Decomposition Tree

OV-5b: Operational Activity Model
SV-10c Systems Event-Trace Description
SV-4 Systems Functionality Description
OV-3: Operational Resource Flow Matrix

Large (> 200 hours to create)

As-Is State
Data Architecture
Other Business Artifacts
Strategic Plan / Con Ops
Transition Strategy
Web Service Description Language (WSDL)
DIV-2: Logical Data Model
DIV-3: Physical Data Model

3.3.2 Across all VA Major Initiatives the Contractor shall:

- Advise VA OIT leadership in support of the Major Initiatives and OneVA EA on future IT Architecture Vision providing a view of what is technologically possible on an implementation-horizon.
- Provide updates and support to Gap, Redundancy and Reuse Analysis. The Gap, Redundancy, and Reuse Analysis identify the investments and adjustments.
- Assist in the development and maturation of existing or new Plan of Action and Milestone (POAM), and other presentation slide decks that promote cost avoidance ideas across OIT. Specifically to review available financial data and pull together financial cost analyses that will help economically justify the idea.
- Support monitoring and tracking of active POAM projects to ensure planned cost avoidance is being realized avoidance across MI Initiatives and One VA EA.

Deliverables:

A. POAM, updated weekly or as specified by VA TOPM
B. Gap, Redundancy and Reuse Analysis
C. Financial Cost Analysis
D. Presentations (using Microsoft Office Suite)
E. SharePoint Site Updates

3.4 INFORMATION TECHNOLOGY APPLIED ARCHITECTURE SUPPORT

Enterprise architecture is an IT discipline that operates in large organizations to further enterprise business goals.

3.4.1 EA Technical Reference Model and Standards Profile (TRMSP)

A Technical Reference Model (TRM) is a component-driven, technical framework categorizing the standards and technologies that support and enable the delivery of EA Service Components and IT capabilities. VA Standards Profile prescribes a set of Technical "Pattern" and best practices for use in Application Development, Network Infrastructure Components, and Server and Database Configurations. Profiles identify applicable standards, permit extensions by and/or restrictions by exception, and provide detailed direction on how to use the clauses, options and parameters of the base standard(s). The Federal Enterprise Architecture (FEA) specifies the use of a TRM and Standard Profiles to unify federal agency and guidance by providing a foundation to advance the reuse and standardization of technology and service components from a government-wide perspective.

The Contractor shall (for **EACH** of the 16 Major Initiatives):

a) Ensure that each major initiative aligns and adhere to the VA TRM.

3.4.2 Proposed Segment Architecture

The FEA is composed of smaller, more focused architecture components termed architecture segments. Architecture Segments are either core mission areas, business services or enterprise service segments – where an enterprise service segment can itself be an enterprise within an enterprise; like the VA is within US Government Federal Enterprise. The VA EA is decomposed in architecture segments along major business lines and critical common IT infrastructure services.

The Contractor shall:

a) Leverage the existing Solution Architecture Framework provided by OneVA EA, FSAM, and FEA to develop solution architectures for each of the 16 Major initiatives. Daily inputs shall be gathered from internal and external IT and business organization regarding potential enhancements and updates using industry Best Practices and experiences. The Contractor shall support monthly updates on the development of proposed solution architecture and identify architecture approval.

Deliverables:

A. VA to FEA Mapping Document

3.4.3 Security Segment Architecture

The VA Security Segment Architecture will represent a view of security related resources, business processes and activities that provide for VA information security.

The Contractor shall:

a) Develop the VA Security Segment Architecture (SSA) making sure it aligns with other existing segments. The Contractor shall gather requirements and recommend best practices for the Security Segment Architecture Model in collaboration with Information Program Resource

Management (IPRM) and provide monthly updates. Segment Architecture will be developed incrementally per prioritized areas of emphasis. The Contractor shall develop briefings, meeting minutes, or other documentation to update and educate stakeholders of the SSA. Monthly updated security architecture models and/or other pertinent SSA documents will be posted to the EA Data Repositories.

b) Ensure the monthly update of the EA Target Architecture Transition Plan includes approved Security Segment Architecture changes. Include content that will address the VA Office of Information Protection and Risk Management (IPRM) perspective in the SSA. The Contractor shall collect requirements and suggest best practices in the identification of new starts or process re-engineering that might be required in order to achieve IPRM guiding principles.

c) Participate in monthly meetings with the Office of IPRM to ensure compliance with existing and new requirements set forth by OIT, and to support and track achievement of IPRM goals. The Contractor shall provide the VA TOPM with minutes of these meetings.

Deliverables:

A. VA Security Segment Architecture
B. Segment architecture expansion plan - in support of the Information Protection and Risk Management offices (IPRM)
C. Segment Architecture education briefings

3.4.4 EA Tool Suite Assessment and Recommendation

The Contractor shall draft a tools assessment that lays out the Contractor's approach, timeline, and tools to be used in execution of the EA Support of the VA's Major Initiatives. The tools assessment should reflect those tools already in use and that are aligned to the EA and Segment EA System Requirements. The assessment shall provide a summary of the results and also the contractor's recommendation regarding which tools best fit the Government's EA requirements. The assessment and recommendation should take into consideration any solution currently being implemented in the VA and other federal agencies, as well as the potential for realizing any possible cost savings to the Government. The Contractor shall also develop and deliver an EA Tool Suite Requirements Implementation Plan for the Major Initiatives based on the Government's final acceptance of recommended EA Tools.

Deliverables:

A. Documented Tools Assessment and Recommendations
B. EA Tool Suite Requirements Implementation Plan

3.4.5 Develop Enterprise Modeling Standards

The Contractor shall define, develop, and document the enterprise architecture modeling standards providing a guide to be used throughout the enterprise. These standards will be used to support

architecture development at the Enterprise, Segment and Solution levels. This standardization will support the Major Initiatives product development, ensuring proper integration with the Segment and Solution tiers. The modeling standards/guide will be used to drive updates to the EA tools and repository to ensure proper architecture development throughout the enterprise. To ensure the implementation of a successful EA suite of tools, the contractor shall introduce querying and reporting functionality to support Major Initiative decision makers, and to provide the Enterprise with architectural meta-model describing the architectural elements extracted from the Major Initiatives.

Deliverables:

A. Enterprise Modeling Guide

4.0 GENERAL REQUIREMENTS

4.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall support VA efforts in accordance with the Program Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

ProPath is a VA-wide process management tool that builds upon the OED Program and Development managers' delivery of high-quality products, and provides an 'at-a-glance' perspective of nearly every step in the software development process. The Contractor shall utilize the tools and templates, and shall file documents in ProPath as a central resource as required by the VA Process.

4.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The following security requirement must be addressed regarding Contractor supplied equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within the VA; Bluetooth must be permanently disabled or removed from the device, c) Equipment must meet all sanitization requirements and procedures before disposal. The

VA TOPM and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

1. Information made available to the Contractor/subContractor by VA for the performance or administration of this contract or information developed by the Contractor/subContractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/subContractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/subContractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and subContractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/subContractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/subContractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA TOPM within 30 days of termination of the contract.
4. The Contractor/subContractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
5. The Contractor/subContractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/subContractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subContractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
7. The Contractor/subContractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
8. The Contractor/subContractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

9. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/subContractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/subContractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA TOPM for response.
10. Notwithstanding the provision above, the Contractor/subContractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/subContractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/subContractor shall immediately refer such court orders or other requests to the VA TOPM for response.
11. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Certification and Accreditation (C&A) or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/subContractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the VA TOPM.
12. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

☒ Low/NACI

☐ Moderate/MBI

☐ High/BI

Position Sensitivity	**Background Investigation** (in accordance with 7010 Handbook Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Minimum Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

Position Sensitivity	Background Investigation (in accordance with 7010 Handbook Appendix A)
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

Contractor Responsibilities:

a) The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language. The Contractor shall provide the name, address, and date of birth, Social Security Number and any other pertinent and relevant information of the Contractor personnel assigned to this project to the VA TOPM prior to Project Kickoff Meeting.
b) The Contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM), the Contractor shall reimburse VA within thirty (30) days.
c) The Contractor shall submit or have their personnel submit the required forms (SF 85P - Questionnaire for Public Trust Positions, SF 85P-S – Supplemental Questionnaire for Selected Positions, FD 258 – U.S. Department of Justice Fingerprint Applicant Chart, VA Form 0710 – Authority for Release of Information Form, Optional Form 306 – Declaration for Federal Employment, and Optional Form 612 – Optional Application for Federal Employment) to the VA Office of Security and Law Enforcement within 30 calendar days of receipt.
d) All costs associated with obtaining clearances for Contractor provided personnel shall be the responsibility of the Contractor. Further, the Contractor shall be responsible for the actions of all individuals provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
e) The Contractor(s) and Contractor point of contact (POC) will receive an email notification from the Security and Investigation Center (SIC) identifying the website link that includes detailed instructions regarding completion of the background clearance application process and what level of background clearance was requested. Reminder notifications will be sent if the complete package is not submitted by the due date.
f) If the security clearance investigation is not completed prior to the start date of the contract, the contract employee may work on the contract with an initiated status while the security clearance is being processed. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for the VA. In the event damage arises from work performed by Contractor personnel, under the auspices of the contract, the Contractor will be responsible for resources necessary to remedy the incident.
g) The investigative history for Contractor personnel working under this contract must be maintained in the databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).

h) The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.
i) Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

4.3 DELIVERABLES

4.3.1 PERFORMANCE METRICS FOR DELIVERABLES

The VA TOPM, with inputs from the VA leads, shall review and accept tasks. Products found to be unacceptable or not meeting the intent of the Task Order shall be redone by the Contractor and considered to be within the scope of this Task Order. To be accepted, deliverables must at least meet the following:

a) There are no oversights in the review and analysis performed by the Contractor that result in incorrect or inadequate assumptions, which, in turn, result in unacceptable recommendations.
b) There are no oversights in the development of reports, documents or functional requirements, which could result in delays in meeting established timelines.
c) All written documentation shall be prepared in a logically organized Contractor format, using paragraph numbers, tables of contents, and page numbers to allow accurate referencing. Documents shall be free from grammatical and typographical errors and shall be formatted in a manner such that paper and printing resources are not wasted. The documentation shall conform to standards for documentation established by VA Lead.
d) The Contractor shall deliver one hard copy and one electronic (PDF Format) copy of all documentation, unless instructed otherwise by the Contracting Officer. In addition to delivering an electronic copy of the documentation, the Contractor shall also post a Microsoft Word version of the documentation to the Contractor Project website within three (3) working days, unless instructed otherwise by the Contracting Officer.
e) All work is completed within the established and agreed upon time frames.
f) The content of deliverables and its work products shall be technically correct, shall reflect VA operating standards, shall reflect PP&C approved processes and procedures, and shall reflect standards of industry.

4.3.2 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise specified by the VA TOPM. Acceptable electronic media include (but not limited to): MS Word 2000/2003/2007, MS Excel 2000/2003/2007, MS PowerPoint 2000/2003/2007, MS Project 2000/2003/2007, MS Access 2000/2003/2007, MS Visio 2000/2002/2003/2007, and Adobe Postscript Data Format (PDF).

4.3.3 SCHEDULE FOR DELIVERABLES

If for any reason, any deliverable cannot be delivered in the time schedule, the Contractor shall provide a written explanation to the VA TOPM who will confer with the GSA COTR and CO. This written transmittal shall include a firm commitment of when the work shall be completed. This notice shall cite the reasons for the delay, and the impact on the overall project. The CO will then review the facts and issue a response in accordance with applicable regulations. The following will be mandatory deliverables for the contract.

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following government work day after the weekend or holiday.

Task	Deliverable ID	Deliverable Description
3.2.1.1	A	**Program Management Plan** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.2	A	**Staff Roster** Due within three business days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.2	B	**Kick-Off Meeting** Within 10 business days after contract.. Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.2	C	**Minutes of Kick-Off Meeting** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.3	A	**Program Communication Plan (one for each of the 16 Major Initiatives)** As agree to with VA TOPM. Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.4	A	**Risk Management Plan (one for each of the 16 Major Initiatives)** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination

3.2.1.4	B	**Risk Status Tracking and Mitigation Reports** Due sixty (60) days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.5	A	**CMP w/Change Control Process (updated)** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.5	B	**CCB Meeting Minutes** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.5	C	**Engineering Change Summaries** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.6	A	**EA WG Charter** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.6	B	**Minutes from EA WG Meetings** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.7	A	**Minutes of IPT Meetings**

		As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.1.7	B	**Written Recommendation** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.2	A	**Weekly Activity Report** Due each Friday throughout the period of performance (PoP). Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.2.2	B	**Monthly Progress Report** Due the fifth day of each month throughout the period of performance (PoP). Electronic submission to: VA TOPM & GSA COTR Inspection: destination Acceptance: destination
3.3.2	A	**Plan of Action & Milestone (POAM)** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.3.2	B	**Gap, Redundancy and Reuse Analysis** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.3.2	C	**Financial Cost Analysis** As agree to with VA TOPM Electronic submission to: VA TOPM

		Inspection: destination Acceptance: destination
3.3.2	D	**Presentations** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.3.2	E	**SharePoint Site Updates** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.2	A	**VA to FEA TRM Mapping Document** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.3	A	**VA Security Segment Architecture** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.3	B	**Segment architecture expansion plan - in support of the Information Protection and Risk Management offices (IPRM)** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.3		**Segment Architecture education briefing** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination

		Acceptance: destination
3.4.4	A	**Documented Tools Assessment and Recommendations** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.4	B	**EA Tool Suite Requirements Implementation Plan** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination
3.4.5	A	**Enterprise Modeling Guide** As agree to with VA TOPM Electronic submission to: VA TOPM Inspection: destination Acceptance: destination

4.4 FACILITY/RESOURCE PROVISIONS

The Government shall provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the VA TOPM as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

The VA shall provide access to VA specific systems/network as required for execution of the task via a site-to-site VPN or other technology, including VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this PWS. The

Contractor shall transmit, store or otherwise maintain sensitive data or products in systems or media other than VA provided systems within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. For detailed Security Requirements refer to ADDENDUM A and B.

4.5 GOVERNMENT FURNISHED PROPERTY

Government furnished equipment and required software: VA will provide all initial access through CITRIX Gateway for all contract workers off-site. Laptops will only be provided to off-site contractors if they are unable to provide tasks, deliverables through CITRIX Gateway. CITRIX Gateway will require VPN access by VA personnel. All Laptops furnished shall be configured by VA personnel. Any specific software requirements for the OneVA EA program development effort will be provided and installed by VA personnel to ensure software is approved and security measures are implemented``. FAR clause 52.245-1 Government Property applies.

5.0 TASK DETAILS & ADMINISTRATION

5.1 Government Management: Task Order Project Manager (TOPM) - The TOPM is a Government (VA) official who has been delegated specific technical, functional and oversight responsibilities for the contract/task order. The TOPM serves as the VA's primary technical point of contact for all contract/task order activities and issues. The TOPM will manage the task order on a day-to-day basis, will review contractor performance and deliverables, and will receive and review all contractor invoices. The TOPM will notify the GSA Contracting Officer's Technical Representative (COTR) of any lapses, problems, or issues. The GSA COTR will notify the Contracting Officer (CO) of problems or issues when warranted.

5.2 Contractor Management: Task Manager (TM) - The Contractor shall designate a single Task Manager to serve as its primary point of contact for all contract/task order activities and issues. The Contractor shall provide sufficient management to ensure that the task is performed efficiently, accurately, on time, and in compliance with the requirements. The Contractor shall coordinate as necessary with the VA TOPM. The Contractor TM shall ensure timely and accurate submission of invoices. The Contractor's TM is responsible for monitoring staff behavior, quality, timeliness, and for providing all administrative oversight of staff assigned to this work

5.3 Task Order Points of Contact - this Performance Work Statement shall be accomplished under the auspices of the General Services Administration (GSA) Federal Acquisition Service, Mid-Atlantic Region:

GSA Contracting Officer
Eileen Flanigan
Phone: (b) (4)
Email: eileen.flanigan@gsa.gov

GSA Contracts Specialist
Ryan Mathews
Phone: (b) (4)
Email: ryan.mathews@gsa.gov

GSA ITM
Allen Cardwell
Phone: (b) (4)
Email: allen.cardwell@gsa.gov

VA Primary Task Order Project Manager (TOPM)
Tracy Pham (**COR**)
810 Vermont Ave. NW (005E)
Washington DC 20420
(b) (4)

VA Alternate Task Order Manager (TOM)
To be designated at time of award

5.4 Performance Details

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO's) for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

5.5 Performance Period

The Period of Performance (POP) shall be one (1) twelve (12) month base period, with four (4) twelve (12) month option period.

Work at the government sites shall not take place on Federal holidays or weekends unless directed by the VA TOPM.

5.6 Place of Performance

Place of performance shall be primarily at the Contractor's facility within the Continental United States (CONUS), using government provided equipment and materials (see Section 4.2 for details). Contractor's facility shall be with 30 mile Proximity to the VA Central Office (VACO) located in Washington, DC.

The Government will not be responsible for the cost for daily on-the-job / local travel.

VA shall provide the necessary software, modeling tools, and repository for the storage, maintenance and delivery of products within the scope of this contract.

Work conducted at VA sites within the CONUS, shall use government provided equipment and materials. This includes the necessary software, hardware, modeling tools, and repository (see Section 4.2 for details).

Work may be performed at remote locations with prior approval of the VA TOPM.

5.7 Travel

The Government anticipates travel under this PWS to attend program-related meetings, conferences, and/or training through the period of performance of this PWS. Travel could be anywhere within the Continental United States (CONUS), however, some anticipated locations include, Salt Lake City, UT, Bay Pines, FL, Austin, TX, Atlanta, GA, Nashville, TN, Tampa, FL, Charleston, SC, Eatontown, NJ and

Kansas City, MO. The anticipated travel shall include two (2) travel request per contractor and a length of four (4) days per trip (per year).

All Travel must be pre-approved by the VA TOPM in advance and in writing. Travel shall be in accordance with the Federal Travel Regulations (FTR).

5.8 Invoice and Billing

The Period of Performance (POP) for each invoice shall be for one calendar month. The contractor shall submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1) The end of the invoiced month (for services) or
2) The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice shall clearly indicate both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor shall submit all required documentation (unless exempted by the contract or order) as follows:

1) For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.
2) For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Posting Acceptance Documents: Invoices shall initially be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the CR (Client Representative, i.e. VA TOPM or designee). Included with the invoice will be all backup documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following options in accepting and certifying services;

1) Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. NOTE: The

Government's preference is that receiving agency's acceptance is conducted electronically.

2) On Paper Copy: The client agency may accept and certify services by providing written acceptance with the signature of the authorized CR and the date of acceptance.

Electronic and/or written acceptance of the invoice by the CR is considered concurrence and acceptance of services. Regardless, of the method of acceptance the contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. (Written acceptances will be posted as an attachment along with any other supporting documentation.) After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted. Although this acceptance may occur in two ways, electronically or in paper copy, at least one shall be obtained prior to the approval of payment. In order to expedite payment, it is strongly recommended that the contractor continue to include the receiving agency's WRITTEN acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If any invoice is received without the required documentation and, (A) the customer's signed written acceptance OR (B) the customer's electronic acceptance, the invoice shall be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor has the option of posting the invoice on GSA's Ft. Worth web site, www.finance.gsa.gov/defaultexternal.asp or mail to the address shown on BLOCK 24 of the GSA FORM 300.

Note: Only use one method of submission, web site or regular U.S. mail, but not both.

Finance Operations and Disbursement Branch (BCEB)
299X
PO Box 219434
Kansas City, MO 641219434
United States

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1) GSA Task Order Number
2) Task Order ACT Number
3) Remittance Address
4) Period of Performance for Billing Period
5) Point of Contact and Phone Number
6) Invoice Amount

7) Skill Level Name and Associated Skill Level Number (for 'Time & Material' or 'Labor Hour' contracts / task orders only)
8) Actual Hours Worked During the Billing Period (for 'Time & Material' or 'Labor Hour' contracts / task orders only)
9) Travel Itemized by Individual and Trip (if applicable)
10) Training Itemized by Individual and Purpose (if applicable)
11) Support Items listed by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, if necessary.

Close-out Procedures

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

Payment Information
The following procedures, if followed, will ensure timely payment of invoices.

Invoice submission is a two-step process:
1) Create an Invoice Acceptance Document in IT-Solutions Shop to obtain Client and GSA Acceptance.
2) Submit the Invoice to GSA Finance either electronically (preferred method), or mail the original invoice to the address stated in the purchase order.

A. To submit your invoice to ITSS for Client Acceptance, follow these steps.

1) Log onto the Internet URL http://web1.itss.gsa.gov.
2) Log into ITSS using your assigned username and password.
3) Once logged in, click on "Create Support Documents".
4) Once in the Create Support Documents field, you will see a list of awarded task order numbers and a pull down menu that reads <<Select Support Document>>. Select the appropriate task order number by highlighting it, then click on the pull down menu; select "Acceptance Information" and click on the "Create" icon.
5) You are now on the page where you will enter the delivery date and invoice number—do not use special characters in the invoice number and be sure to use exactly the same invoice number and value for GSA Finance. You have the opportunity to send comments to the client (receiving activity) in the detailed comments block. You must attach an electronic copy of your invoice. Click on the thumbtack "Attach" icon to bring up the attachments page. When you are done attaching the invoice, click on the "Submit" button at the bottom of the page to complete the process.

When the acceptance document is submitted, emails requesting acceptance are automatically sent to both the Client and the GSA Information Technology Manager (ITM). They will accept, partially accept, or

reject the invoice, normally with explanatory comments. The Client will also indicate the amount approved for payment. The system will automatically notify you, the Vendor, of acceptance or rejection of the invoice.

If you need assistance or have any questions regarding the acceptance and approval process, please contact the ITSS Help Desk at the toll free number 1-877-243-2889. Be sure to have the order number or act number available.

B. AFTER (and only AFTER) you receive acceptance through ITSS, you must then submit your invoice to the GSA Finance Office for payment, using ONE of the following two methods. DO NOT DO BOTH.

Method 1 – Electronic Submission (This is the preferred method)
If you do not have a password, go to www.finance.gsa.gov and click on "Get a Password for Payment Searches" under "Quick References" on the left side of the screen. Fill out the form and submit. You should receive your password within 24 hours.

1) Log into the GSA Finance website at www.finance.gsa.gov.
2) Click on "Click here to Login".
3) Enter your password* and click "login Do not use the "Enter key". Use the mouse to click on "Login." Using "cut and paste" may not work; you may need to type your password which is not case sensitive.
4) Select "submit invoice".
5) Select "All POs".
6) Find the ACT# or PDN# you are invoicing against and select it. A form will appear that you fill in with your invoice information. Be sure to use the same invoice number (do not use special characters) and value which you used in the ITSS Acceptance document. If you are resubmitting a rejected invoice, add an "R" or an "A" to the end of the original invoice number or use an entirely new invoice number. The GSA system will not let you use an invoice number you have used before.
7) Fill in the information requested. All fields marked with an asterisk (*) are required fields.
8) When complete, click "continue". If you have made any errors, you will receive an error message. (Worth noting: dates are in mm/dd/yyyy format, money amounts have no $ signs or commas, only a decimal point.) Correct the error and click "continue" again.
9) You will have an opportunity to upload any backup material as attachments after clicking "submit" on the next screen.
10) Add any invoice backup material as attachment.

1. If you have questions please e-mail FW-PaymentSearch.finance@gsa.gov or call the Customer Support Desk at 1-817 / 978 2408. Anyone there will be able to assist you.

Method 2 – Hard Copy Submission

1) Return to the ITSS "Acceptance Information" page (per the above instructions) and print the page showing the client's acceptance.
2) Mail your original invoice (on official company letterhead), accompanied by the client's acceptance page, to the GSA Finance Office in Ft Worth, at the address shown in Block 24 (below) of this document. Please ensure that the GSA Delivery Order Number and the ACT Number (found in Blocks 2 and 4 of this GSA Form 300, respectively) are clearly shown on your invoice.

C. To check the payment status of an invoice, go to www.finance.gsa.gov**.** Click on "Click here to Login" Enter your password and click "login. DO NOT USE THE ENTER KEY. USE THE MOUSE TO CLICK ON "LOGIN". Please note that using "cut and paste" may not work. You may need to type your password which is not case sensitive.

1) Select "Payment Search". This shows paid invoices.
2) If your invoice is not there, select "View Invoice", then "all unpaid invoices". (You may also select "search unpaid" and enter specific criteria to narrow the search.)
3) If your invoice is not there, back up one page and select "all rejected invoices" under "View Invoice". (You may also select "search rejected" and enter specific criteria to narrow the search.)

Remember that once an invoice shows in the "rejected invoices" section, it will always be there. They do not disappear when an invoice is resubmitted and paid. Your invoice could appear in this section multiple times if rejected multiple times.

If you have questions please e-mail FW-PaymentSearch.finance@gsa.gov or call the Customer Support Desk at 817 978 2408. Anyone there will be able to assist you.

6.0 APPLICABLE DOCUMENTS / CLAUSE

6.1 DOCUMENTS

Documents referenced or germane to this PWS are listed below. The documents have been designated as either mandatory or informational. Additional documents may be specified in the individual task order.

In the performance of the tasks Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
3. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," September 10, 2004
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12)

15. VA Directive 6500, "Information Security Program," August 4, 2006
16. VA Handbook 6500, "Information Security Program," September 18, 2007
17. VA Handbook 6500.6, "Contract Security," March 12, 2010
18. NBS SP500-153, "Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach," April 1988
19. Program Management Accountability System (PMAS) portal (reference Vendor Library at http://www1.va.gov/oamm/oa/tac/)
20. OED ProPath Process Methodology (reference Vendor Library at http://www1.va.gov/oamm/oa/tac/) NOTE: In the event of a conflict, OED ProPath takes precedence over other processes or methodologies.
21. Technical Reference Model (TRM) (reference Vendor Library at http://www1.va.gov/oamm/oa/tac/)
22. National Institute Standards and Technology (NIST) Special Publications
23. VA website at www.va.gov
24. OneVA website at http://www.ea.oit.va.gov/
25. VA Directive 6051 at http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=3&FType=2
26. OneVA Enterprise Architecture Guidance at http://www.ea.oit.va.gov/extdocs/EAGuideSigned.pdf
27. IPRM Guiding Principles at http://www.iprm.oit.va.gov/index.asp
28. VA Directive 6330 at http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=430&FType=2
29. VA Handbook 6330 at http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1813
30. US Title 5 Section 6103 at http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t05t08+700+0++()%20%20AND%20
31. Project Management Accountability System (PMAS) Guide at http://vaww.ppoe.oit.va.gov/docs/PMAS_Guide_March_29_2010.pdf
32. Project Management Institute – Project Management Body of Knowledge at www.pmi.org
33. OI&T Process Library at http://vaww.oed.wss.va.gov/process/Library/oed_propath_process_home.pdf

6.2 FAR CLAUSES

FAR 52.245-1 - Government Property

FAR 52.224-1 - "Privacy Act Notification" and 52.224-2 - "Privacy Act" apply to this contract.

VAAR 852.273-75 - Security Requirements for Unclassified Information Technology Resources (Interim - OCT 2008)

FAR52.239-1 Privacy or Security Safeguards (Aug. 1996)

FAR 52.222-54 Employment Eligibility Verification (Jan. 2009)

FAR 52.204-9 - Personal Identity Verification of Contractor Personnel

1) The contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12

(HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

2) The contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system

FAR 52.237-3 - Continuity of Services

Pursuant to FAR Clause 52.237-3 - Continuity of Services (JAN 1991) (DEVIATION – MAY 2003), the contractor shall comply with the following:

1) The contractor recognizes that the services under this contract are vital to the ordering activity and must be continued without interruption and that, upon contract expiration, a successor, either the ordering activity or another contractor, may continue them. The contractor agrees to-

    i) Furnish phase-in training; and
    ii) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

2) The contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.
3) The contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.
4) The contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.[1] The Contractor's firewall and web server shall meet or exceed the VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://vaww.eas.vaco.va.gov/OneVAEA/ in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). The VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508.

[1] See VAAR 852.273-75 referenced *infra*.

These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http//www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self contained, closed products
_x_ § 1194.26 Desktop and portable computers

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. The VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. The VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of the VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this PWS, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by the VA.
7. Contractor must adhere to the following:
8. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.

12. VA, as well as any Contractor (or Contractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
13. Contractor TM and VA TOPM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

A6.0 SUBPART 839.2 – INFORMATION AND INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

839.201 Contract clause for Information and Information Technology Security:

a. Due to the threat of data breach, compromise or loss of information that resides on either VA-owned or contractor-owned systems, and to comply with Federal laws and regulations, VA has developed an Information and Information Technology Security clause to be used when VA sensitive information is accessed, used, stored, generated, transmitted, or exchanged by and between VA and a contractor, subcontractor or a third party in any format (e.g., paper, microfiche, electronic or magnetic portable media).

b. In solicitations and contracts where VA Sensitive Information or Information Technology will be accessed or utilized, the VA TOPM shall insert the clause found at 852.273-75, Security Requirements for Unclassified Information Technology Resources.

A7.0 852.273-75 - SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (INTERIM- OCTOBER 2008)

As prescribed in 839.201, insert the following clause:

The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

ADDENDUM B

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B1. GENERAL

Contractors, Contractor personnel, subContractors, and subContractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a) A Contractor/subcontrator shall request logical (technical) or physical access to VA information and VA information systems for their employees, subContractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b) All Contractors, subContractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c) Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d) Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/subContractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e) The Contractor or subContractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the

Contractor or subContractor's employ. The Contracting Officer must also be notified immediately by the Contractor or subContractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

a) Information made available to the Contractor or subContractor by VA for the performance or administration of this contract or information developed by the Contractor/subContractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/subContractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b) VA information should not be co-mingled, if possible, with any other data on theContractors/subContractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and subContractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c) Prior to termination or completion of this contract, Contractor/subContractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/subContractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d) The Contractor/subContractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e) The Contractor/subContractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/subContractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subContractor needs to be restored to an operating

state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f) If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g) If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h) The Contractor/subContractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i) The Contractor/subContractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j) Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/subContractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/subContractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k) Notwithstanding the provision above, the Contractor/subContractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/subContractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/subContractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l) For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the Contractor/subContractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the VA TOPM.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a) Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and

related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the VA TOPM, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b) The Contractor/subContractor shall certify to the VA TOPM that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c) The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

d) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e) The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f) The Contractor/subContractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

g) The Contractor/subContractor agrees to:

   (a) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

      i. The Systems of Records (SOR); and

      ii. The design, development, or operation work that the Contractor/subContractor is to perform;

(b) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

(c) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts

h) awarded under this contract which requires the design, development, or operation of such a SOR. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/subContractor is considered to be an employee of the agency.

(a) "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

(b) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(c) "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

i) The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

j) The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than ____ days.

k) When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible

for operations or maintenance of the Systems, they shall apply the Security Fixes within ____ days.

l) All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a) For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/subContractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the VA TOPM and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b) Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c) Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d) The Contractor/subContractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The Contractor/subContractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government.

Contractor/subContractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/subContractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e) The Contractor/subContractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the VA TOPM. The government reserves the right to conduct such an assessment using government personnel or another Contractor/subContractor. The Contractor/subContractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f) VA prohibits the installation and use of personally-owned or Contractor/subContractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g) All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/subContractor or any person acting on behalf of the Contractor/subContractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/subContractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/subContractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h) Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

    a. Vendor must accept the system without the drive;

    b. VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

i. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

ii. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

iii. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

a) The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/subContractor shall immediately notify the VA TOPM and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subContractor has access.

b) To the extent known by the Contractor/subContractor, the Contractor/subContractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subContractor considers relevant.

c) With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d) In instances of theft or break-in or other criminal activity, the Contractor/subContractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its

employees, and its subContractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subContractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a) Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/subContractor processes or maintains under this contract.

b) The Contractor/subContractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c) Each risk analysis shall address all relevant information concerning the data breach, including the following:

    a. Nature of the event (loss, theft, unauthorized access);

    b. Description of the event, including:

        i. date of occurrence;

        ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

    c. Number of individuals affected or potentially affected;

    d. Names of individuals or groups affected or potentially affected;

    e. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

    f. Amount of time the data has been out of VA control;

g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

h. Known misuses of data containing sensitive personal information, if any;

i. Assessment of the potential harm to the affected individuals;

j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

k. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d) Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of $_____ per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

a. Notification;

b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

c. Data breach analysis;

d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

e. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

f. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

a) All Contractor employees and Sub-Contractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

   a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;

   b. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;

   c. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

   d. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access ***[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]***

b) The Contractor shall provide to the contracting officer and/or the VA TOPM a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c) Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.